ZERO TRUST AUDIT CHECKLIST

Zero Trust & Post-Quantum Readiness

Standard: NIST SP 800-207 + CISA ZTMM **Date:** 2026-08-15 **Confidential**

Every control below requires evidence (tool output, configuration, logs) before it may be marked PASS. Scale:

PASS PARTIAL FAIL N/A UNVERIFIED — needs internal review

A · PERIMETER GATE (EXTERNALLY VERIFIABLE)

#	CONTROL	STATUS	EVIDENCE
A1	Admin console default-deny — unauthenticated access redirects to login	PASS	/console/ → 302 / admin-gate/ login.php
A2	Origin hidden — DNS exposes only the shield, not the origin	PASS	A record = shield IP
A3	No sensitive files exposed (.git, .env, backups, wp-admin, actuator)	PASS	403/404 responses
A4	No version leak in content	PASS	HTML scan
A5	Security headers complete (HSTS, CSP, nosniff, frame, referrer, permissions)	FAIL	All missing — see hardening config
A6	Stack/fingerprint headers minimized (server, via, x-powered-by)	FAIL	server: LiteSpeed · via: Caddy
A7	TLS floor 1.2+ (no 1.0/1.1)	PASS	1.2 & 1.3 only
A8	TLS 1.3 + PQC hybrid key exchange (X25519MLKEM768)	PASS	Negotiated by default
A9	TLS 1.2 disabled (force PQC-capable connections)	PARTIAL	1.2 still active
A10			

	Sensitive paths return 404 (not 403)	PARTIAL	/.git, /.env → 403

B · IDENTITY & ACCESS (INTERNAL REVIEW — CONSOLE)

#	CONTROL	STATUS	EVIDENCE REQUIRED
B1	MFA/2FA (TOTP or WebAuthn) for console	UNVERIFIED	login config / IdP
B2	Strong password policy + rotation	UNVERIFIED	Policy document
B3	Rate limiting / lockout anti brute-force on login	UNVERIFIED	fail2ban / server built-in
B4	CSRF token on login form	UNVERIFIED	Source code
B5	Session cookie flags: HttpOnly; Secure; SameSite	UNVERIFIED	Response headers post-login
B6	Session expiry + rotation	UNVERIFIED	Config
B7	RBAC — role-based access to console/API	UNVERIFIED	User matrix
B8	Account provisioning/deprovisioning (offboarding)	UNVERIFIED	SOP
B9	Login audit log (success/fail, IP, timestamp)	UNVERIFIED	Server logs
B10	Per-request authorization (not one-time auth only)	UNVERIFIED	Policy engine

C · DEVICE POSTURE (INTERNAL REVIEW)

#	CONTROL	STATUS	EVIDENCE REQUIRED
C1	Device attestation / posture check before access	UNVERIFIED	ZTNA config
C2	mTLS / client certificates for service access	UNVERIFIED	Gateway/TLS config
C3	Endpoint security requirement (EDR/AV)	UNVERIFIED	Policy
C4			

	Lost/stolen device revocation	UNVERIFIED	SOP + CRL

D · SEGMENTATION & MICRO-SEGMENTATION

#	CONTROL	STATUS	EVIDENCE REQUIRED
D1	Origin not directly reachable (firewall allows only shield IP)	UNVERIFIED	iptables/nftables on origin
D2	Service-to-service mTLS / network policy	UNVERIFIED	Service mesh / rules
D3	No lateral access between zones (DMZ/ internal/db)	UNVERIFIED	Topology + rules
D4	API token auth per service, not blanket access	UNVERIFIED	Gateway config
D5	Internal DNS not exposed publicly (split-horizon)	UNVERIFIED	DNS config

E · DATA PROTECTION (PQC & ENCRYPTION)

#	CONTROL	STATUS	EVIDENCE REQUIRED
E1	PQC hybrid TLS (X25519MLKEM768) enabled	PASS	openssl s_client
E2	Pure ML-KEM (future option) — hybrid recommended	N/A	—
E3	Encryption at rest (disk + DB + backups)	UNVERIFIED	LUKS/encrypted FS, DB TDE
E4	Key management: rotation, vault/HSM, least privilege	UNVERIFIED	Vault/HSM config
E5	PQC certificates (ML-DSA) — monitor ISRG/Let's Encrypt	N/A	No public provider yet
E6	Data minimization + retention (PDPA)	UNVERIFIED	DPA + retention policy

F · CONTINUOUS VERIFICATION & ANALYTICS

#	CONTROL	STATUS	EVIDENCE REQUIRED

F1	Complete access logging (who, what, when, from where)	UNVERIFIED	Gateway + app logs
F2	Monitoring/anomaly detection (login-failure spikes etc.)	UNVERIFIED	SIEM/Wazuh/ Prometheus
F3	Alerting + escalation path	UNVERIFIED	Incident SOP
F4	Log retention + integrity (append-only / hashing)	UNVERIFIED	Log config
F5	Scheduled testing (VAPT) + remediation	UNVERIFIED	Test reports

G · POLICY ENGINE & AUTOMATION

#	CONTROL	STATUS	EVIDENCE REQUIRED
G1	Per-request access decisions (not network-trust based)	UNVERIFIED	ZTNA policy engine
G2	Central, versioned policy (IaC)	UNVERIFIED	Ansible/Terraform
G3	Automated incident response (isolate device/service)	UNVERIFIED	Runbook + automation
G4	Zero standing privileges (JIT access)	UNVERIFIED	PAM config

REMEDIATION PRIORITIES (FINDINGS 2026-08-15)

P1 — This week (easy, high impact)

- Add security headers at the gateway layer — HSTS, CSP, nosniff, DENY frame, referrer, permissions (A5).
- Strip **via: Caddy** and minimize the **server:** header — reduce fingerprinting (A6).

P2 — 30 days

- Harden the login gate: MFA + rate limiting + CSRF + cookie flags (B1–B6).
- Origin isolation: firewall on the origin accepts only the shield IP (D1).
- Disable TLS 1.2 if the client base supports 1.3 (A9).

P3 — Quarterly

- mTLS + device posture for internal access (C2, C1).
- PQC certificate chain when providers support it (E5) — monitor ISRG/Let's Encrypt.
- Scheduled audits + log integrity (F1–F5).

UNVERIFIED items require evidence from internal review (configuration, logs, SOPs). This checklist is a list of evidence to collect — not a claim of compliance.
